eBook

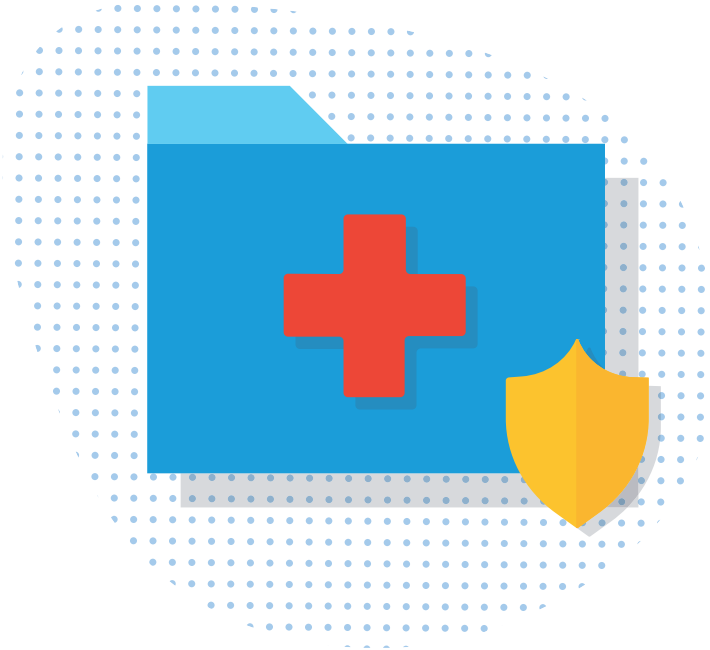
Healthcare Company? Cure Your IT Ailments with Business Continuity

As a healthcare company, your patients are your number one priority. Part of your obligation to them is to keep their health-related information as confidential as possible.

This information can include the patient's health history, insurance details, and financial information. Should any of this information be compromised, it can hinder your ability to deliver healthcare services.

Healthcare regulations are constantly evolving and, in order to meet new industry standards, more and more healthcare businesses are actively converting medical records into electronic versions.

As this trend continues, it's no surprise that the industry has been hit hard recently by cyber attacks. Entire systems can fall victim to ransomware, locking healthcare providers out of important patient data. The companies affected are paying huge sums to recover. As people's lives can quite literally depend on a healthcare provider's ability to access their health information, there isn't any time to waste.



Keeping your patient data properly backed up and protected will help you focus on what matters – the patients you care for.

A False Sense of Security

While you may be taking some precautions, such as securing and backing up your sensitive data, sometimes that's not enough. There is a common misconception that data is safe if backed up once a day, but this outdated practice is no longer sufficient for several reasons:

- If you forget to perform the backup or the backup process fails, you're not protected.
- If you only back up your files once a day, you're left vulnerable to the loss of an entire day's work.
- If you don't properly validate your backup files, you could be in for an unpleasant surprise when you actually try to use those files to restore your company's operations.
- If you only back up your files on-site, you could lose them too – leaving you with no way to meet client requests.

If you only back up your raw data, rather than all your application and server configuration files, it could take several days to restore your practice – because you will also have to rebuild your servers, operating systems, applications, etc. Ultimately, there's a lot that can be missed when implementing a backup strategy, so it's important to get it right the first time around. Keeping your patient data properly backed up and protected will help you focus on what matters the patients you care for.

Healthcare data breach costs average $408 per record, the highest of any industry.

How Vulnerable Are You?

If your company identifies as a business that doesn't have the IT resources to effectively recover from a major outage, make sure you're weighing all of the factors around the costs of downtime. Here are the facts:

- US businesses lose $12 billion annually due to data loss.[1]
- 93% of companies that lose their data center for 10+ days file for bankruptcy within one year.[2]

Best Practices for Healthcare IT

According to a 2018 study by IBM and the Ponemon Institute, healthcare data breach costs average $408 per record, the highest of any industry for the eighth straight year and nearly three times higher than the cross-industry average of $148 per record.[3] Attacks on the healthcare industry are clearly on the rise, but there are some precautions you can take to safeguard your data:

- **Outsource your company's IT needs to an expert who has experience in the healthcare industry.**
  - Look for a company educated in HIPAA with a team that's dedicated to security and compliance.
  - Ask for references so you can hear from fellow healthcare professionals about their experience with the company.

Any company that has not recently re-assessed its backup and disaster recovery procedures should do so in order to conform to the industry-standard best practices.

- **Don't sacrifice quality to save money when purchasing hardware. It will benefit you (and your bottom line) to have strong technology in the long run.**
- **Perform timely hardware and software updates, maintenance and backups.**
- **Establish, review and maintain system security of all practice technology.**

Any company that has not recently re-assessed its backup and disaster recovery procedures should do so in order to conform to these industry - standard best practices.

Take it from a healthcare company who has dealt with a fair share of attacks to their data. When their pharmacy fell victim to a destructive robbery, the team at Complete Pharmacy Care was able to get back to business thanks to their business continuity solution.

"Because of the physical damage, had we not been on the cloud we absolutely would have gone bankrupt because it would have taken us six weeks to rebuild all of the equipment. But because we could get on the cloud, we brought in laptops and dialed into the cloud and were able to start servicing patients by Tuesday. We were able to start serving patients on a limited basis on Tuesday. We were only down one day. Had we not had a second copy of our data already up in the cloud, we would not be having this conversation."
– Leonard Lynskey, CEO, Complete Care Pharmacy.

The Better Way: Business Continuity

Business continuity describes a complete solution for backup and disaster recovery. A true business continuity solution will protect data on-premises and in the cloud. Whether data is on servers or in SaaS applications, it needs to be backed up. Business continuity goes a step further and offers you the ability to restore your data, which we call disaster recovery.

Whether a business is faced with a natural disaster or one man-made, a strong solution will have you up and running in minutes. Solutions that leverage the hybrid cloud can guarantee a quicker restore time as well.

Why? Local backups are great to keep data stored on local devices, but if something happens to that device, then what? A hybrid cloud backup solution takes an initial backup on a local device and then replicates the backup to a cloud server. Cloud-only solutions are not as reliable on their own due to bandwidth issues. A hybrid model works to alleviate the vulnerabilities by implementing both processes to fill in the gaps. That's intelligent business continuity.

Unified Network Group
Relax, we got IT.

For more information please contact:
pPhone: 864.278.0202
https://www.unifiednetworkgroup.com

Sources

[1] Beyond Technology
[2] National Archives & Records Administration
[3] The Ponemon Institute